VISCHER

GLOSSAR PRIVACYSCORE.CH

Audit Trail	Eine Massnahme der Datensicherheit, bei welcher alle relevanten Schritte, die ein Benutzer in einem Computersystem vornimmt (Einloggen, Änderungen, Übermittlungen, Abrufe etc.) protokolliert werden, damit sie später nachvollzogen werden können.
Auftragsbearbeiter	Das sind Stellen (i.d.R. Unternehmen), die im Auftrag eines Verantwortlichen dessen Datenbearbeitung durchführen und selbst nicht entscheiden, wie dies im Wesentlichen zu geschehen hat (d.h. sie sind weisungsgebunden tätig). Hierzu gehören z.B. viele IT-Service-Provider. In der DSGVO heisst der Auftragsbearbeiter "Auftragsverarbeiter", was dasselbe meint.
AVV, ADV, DPA	Der Vertrag ("Auftragsverarbeitungsvertrag", manchmal auch "ADV" oder "DPA" genannt), den ein Verantwortlicher mit seinem Auftragsbearbeiter abschliesst, um den datenschutzrechtlichen Anforderungen zu genügen. Er sieht u.a. vor, dass der Auftragsbearbeiter nur auf Weisungen des Verantwortlichen handelt, eine angemessene Datensicherheit sicherstellen und die Daten am Ende wieder löschen muss.
BCR	Binding Corporate Rules, eine Möglichkeit, mit welcher Unternehmensgruppen den Datenfluss zwischen den einzelnen Gesellschaften datenschutzrechtlich so regeln können, dass die Daten auch dann fliessen dürfen, wenn eine Gesellschaft sich in einem Land ohne angemessenen Datenschutz befindet. Es sind im Wesentlichen konzernweite Datenschutzverträge. Die meisten Unternehmen setzen jedoch auf ein IGDTA, weil dieses einfacher zu realisieren ist und keine behördliche Genehmigung erfordert.
Bearbeitungsgrundsätze	Es sind dies eine Reihe von Grundregeln, die das DSG und die DSGVO für den datenschutzkonformen Umgang mit Personendaten festgelegt haben, wie namentlich den Grundsatz der Transparenz, der Zweckbindung, der Verhältnismässigkeit (einschliesslich der Datenminimierung und der Begrenzung der Aufbewahrungsdauer), der Datenrichtigkeit, der Datensicherheit, der Fairness der Datenbearbeitung bzw. den Grunsatz von Treu und Glauben, und die Rechtmässigkeit der Datenbearbeitung.
Besonders schützenswerte Personendaten	Im DSG sind dies Personendaten, (i) über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigen, (ii) über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, (iii) genetische Daten, (iv) biometrische Daten, die eine natürliche Person eindeutig identifizieren, (v) über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen, und (vi) über Massnahmen der sozialen Hilfe. Für sie gelten besondere Vorgaben. In der DSGVO ist der Katalog dieser Daten ähnlich definiert: Es sind dies Personendaten, (i) aus denen die rassische und ethnische Herkunft, (ii) politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, (iii) genetischen Daten, (iv) biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, (v) Gesundheitsdaten und (vi) Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Hinzugerechnet werden oft auch (vii) Daten über strafrechtliche Verurteilungen und Straftaten und (viii) über damit zusammenhängende Sicherungsmassregeln.
Bearbeiten	Meint jeden Umgang mit Personendaten, wie z.B. das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. In der DSGVO ist von "Verarbeiten" die Rede, was dasselbe meint.
Bearbeitungsverzeichnis	Das Verzeichnis der Bearbeitungsaktivitäten, kurz Bearbeitungsverzeichnis oder Records of Processing Activities genannt. Teilweise wird auch der Begriff Verfahrensverzeichnis benutzt. Es bietet einen Überblick über die einzelnen Datenbearbeitungen eines Unternehmens an. Das DSG und die DSGVO schreibt es in gewissen Fällen vor.

BYOD	Bring-you-own-Device, das von immer mehr Unternehmen genutzte Konzept, dass Mitarbeitende die Geräte, die sie für ihre Arbeit benötigen, selbst bereitstellen, z.B. indem sie ihr privates Mobiltelefon benutzen, um geschäftliche E-Mails abzurufen.
CMP	Consent Management Platform, die Bezeichnung für eine Softwarelösung, mit welcher Unternehmen die Besucher ihrer Websites um ihre Einwilligung in das Tracking bzw. Setzen von Cookies bitten können.
Cookies	Cookies ist eine sehr alte Technik, mit welcher der Betreiber einer Website seinen Server so programmieren kann, dass er jedem Besucher ein digitales Etikett (das "Cookie") mit einer Nummer übermittelt. Kommt der Besucher später zur Website zurück, kann er ihn anhand der Nummer als früheren Besucher wiedererkennen. Wer der Besucher ist, weiss er damit aber noch nicht. Cookies werden benutzt, um Besucher auf Websites zu tracken, was wiederum Analysezwecken dient oder um Interessen zu ermitteln, was dann für gezieltere Werbung benutzt werden kann.
DLP	Data Loss Prevention, eine Massnahme der Datensicherheit, um unerwünschten "Abfluss" von Unternehmensdaten zu verhindern, indem z.B. E-Mails daraufhin gescannt werden, ob sie Geschäftsgeheimnisse enthalten oder z.B. die Verwendung von USB-Sticks an Computern gesperrt wird, damit Mitarbeitende oder Dritte keine Daten entwenden können.
DMZ	Demilitarisierte Zone, ein im Zusammenhang mit Firewalls benutzter Fachbegriff. Er beschreibt einen digitalen "Vorhof" zu einem Unternehmensnetzwerk, in welchem sich Besucher aufhalten können, aber nicht ins Innere des Unternehmensnetzwerks gelassen werden. Wer ein WLAN einrichtet und es Gästen zur Verfügung stellen will, kann es so programmieren, dass diese es zwar nutzen können, aber von dort aus nicht auf den Rest der Firma zugreifen können; sie müssen quasi in der DMZ bleiben.
DSE	Die Datenschutzerklärung, die beschreibt, was ein Verantwortlicher an Personendaten erhebt, was er damit wie tut und welche Rechte die betroffene Person hat. Das DSG und die DSGVO schreiben sie in vielen Fällen vor.
DSFA	Datenschutz-Folgenabschätzung, d.h. die dokumentierte Prüfung, ob ein geplantes Vorhaben bezüglich der bearbeiteten Personendaten unerwünschte negative Konsequenzen für die betroffenen Personen haben kann, und welche Massnahmen dagegen ergriffen werden. DSG und DSGVO schreiben eine solche Prüfung in gewissen Fällen vor.
DSG	Datenschutzgesetz, wie es in der Schweiz den Datenschutz für den privaten Sektor und Bundesorgane regelt. Weiter gibt es noch kantonale und kommunale Datenschutzgesetze, die aber nur für öffentliche Organe in den Kantonen und Gemeinden gelten.
DSGVO	Die Datenschutz-Grundverordnung der EU und des Vereinigten Königreichs. Es ist das Gegenstück zum DSG und regelt den Datenschutz im EWR. Das Vereinigte Königreich hat die DSGVO schon vor dem Brexit übernommen.
EDR	Endpoint Detection & Reponse, eine Massnahme der Datensicherheit, bei welcher auf den Endgeräten (z.B. Notebook) ein Programm installiert wird, das auf verdächtiges Verhalten achtet und Alarm schlägt bzw. Zugriffe sperrt, wenn ein Cyberangriff oder sonst eine missbräuchliche Nutzung vermutet wird.
EU SCC	Die Standardvertragsklauseln (Standard Contractual Clauses) der Europäischen Kommission. Gemeint ist damit i.d.R. der Standardvertrag, den die Europäische Kommission freigegeben hat für die Absicherung von Datenübermittlungen in Staaten, die über kein angemessenes Datenschutzniveau verfügen. Diese können mit entsprechenden Modifikationen auch unter dem DSG benutzt werden.
IGDTA	Intra-Group Data Transfer Agreement, ein gruppeninterner Vertrag, der den Datenfluss innerhalb einer Unternehmensgruppe in datenschutzrechtlicher Hinsicht regelt.

ISMS	Informationssicherheits-Management-System, ein strukturiertes Vorgehen in einem Betrieb, um die Massnahmen zur Sicherstellung der Informationssicherheit richtig zu definieren, ihre Umsetzung sicherzustellen und dafür zu sorgen, dass sie bei Bedarf verbessert, ersetzt oder ergänzt werden. Ein ISMS besteht u.a. aus Prozessen, Weisungen, der Zuweisung von Verantwortlichkeiten, Risikobeurteilungen und Dokumentation. Es folgt oft einem Standard, wie z.B. ISO 27001 und kann in diesen Fällen auch "zertifiziert" werden. Die getroffenen Massnahmen (TOMS) sind das Ergebnis, aber nicht Teil des ISMS.
MDM	Mobile Device Management, d.h. eine Disziplin der IT bzw. Datensicherheit, um mobile, ans Unternehmensnetzwerk angeschlossene Geräte zu verwalten und für die Sicherheit zu sorgen.
MFA, ZFA	Multi-Faktor-Authentifizierung, oder auch Zwei-Faktor-Authentifizierung (2FA), bezeichnet alle Verfahren, bei denen die Prüfung der Zugriffsberechtigung nicht nur durch ein einzelnes Passwort oder sonst einen einzigen sicheren "Faktor" erfolgt (nebst dem Benutzernamen), sondern durch zwei oder mehr, also durch ein per SMS übermittelter Code, durch einen Fingerabdruck oder durch die Verwendung einer Authenticator-App. Dies ist eine wesentliche Sicherheitsmassnahme. Fehlt sie, kann jeder, der an das Passwort eines Benutzers gelangt, sich mit diesem Zugang zu seinem Konto verschaffen, schlimmstenfalls ohne, dass er es merkt.
Personendaten	Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Es muss also möglich sein, die Person, auf welche sich die Daten beziehen, mit vernünftigen Mitteln identifizieren zu können, sei es direkt (z.B. durch den Namen, ein Bild oder eine Telefonnummer) oder indirekt (z.B. durch eine Internet-Recherche). In der DSGVO ist von "personenbezogenen Daten" die Rede, was dasselbe meint.
Profiling	Gemeint eine vollautomatisierte Bewertung einer Person durch einen Computer, d.h. ein Wertentscheid (z.B. Prognose, Einschätzung) bezüglich einer Eigenschaft (z.B. Interesse) oder eines Verhaltens einer einzelnen Person aufgrund deren Personendaten.
ROPA	Records of Processing Activities, das Bearbeitungsverzeichnis.
TIA	Transfer Impact Assessment, die dokumentierte Prüfung, ob im Falle einer Übermittlung von Personendaten in ein fremdes Land die dortigen Behörden Zugriff auf diese erlangen könnten und ob dies in einer Art und Weise geschehen kann, die nach europäischem Verständnis problematisch wäre. DSG und DSGVO schreiben eine solche Prüfung in gewissen Fällen vor.
TOMS	Technische und organisatorische Massnahmen der Datensicherheit; dies ist der Überbegriff für all die Vorkehrungen, die ein Betrieb unternimmt, um die Datensicherheit zu gewährleisten, und zwar sowohl in technischer Hinsicht (z.B. Firewalls, Verschlüsselung) wie auch in organisatorischer Hinsicht (z.B. Weisungen, Schulungen, Verträge).
Verantwortlicher	Diejenige Stelle (i.d.R. ein Unternehmen), welche im Wesentlichen festlegt, wozu oder wie Personendaten bearbeitet werden und die daher für die Einhaltung des Datenschutzes diesbezüglich verantwortlich ist. Eine Datenbearbeitung kann zugleich mehrere Verantwortliche haben, die zusammen über eine Bearbeitung entscheiden oder jeweils über bestimmte Aspekte.

11.3.2023